III. REMARKS

1.   Claims 1-20 and 22-26 remain in the application.   Claim 21 has been cancelled.   Claims 27-30 have been withdrawn.

2.   Applicants respectfully submit that claims 1-12 are patentable over the combination of Kuhn, *Probability Theory For Pickpockets-ec-PIN Guessing*, August 30, 1997, ("Kuhn") in view of Matyas et al. (US 4,924,514 "Matyas").

The combination of Kuhn and Matyas fails to disclose or suggest a method for generating a pin as recited in claim 1.

Kuhn, on page 1, lines 12-17 describes how a bank calculates a customer PIN using the following steps:

> forming a 16 digit decimal number by concatenating five digits of a bank routing number, a ten digit account number, and a single digit card sequence number;

> transforming the concatenation into a 64 bit pattern by encoding each digit with its 4 bit BCD equivalent;

> encrypting the 64 bit BCD equivalent result using the DES algorithm with a 56 bit key (K_1);

> representing the 64 bit result as a 16 digit hexadecimal number; and

> "decimalizing" digits 3-6 of the 16 digit hex number by substituting all occurrences of letters A-F with numbers 0-5 respectively to form a 4 digit PIN.

2.1 The Examiner states that the steps of concatenating the five digits of the bank routing number, the ten digit account

7

number, and the single digit card sequence number; transforming the concatenation into a 64 bit pattern by encoding each digit with its 4 bit BCD equivalent; and encrypting the 64 bit BCD equivalent result using the DES algorithm with a 56 bit key (K_1) equates to Applicants' generating a number of random binary bits.

Applicants respectfully disagree because the combination of Kuhn and Matyas, and in particular Kuhn's process will yield the same result each time it is performed. As long as the same five digits of the bank routing number, the same ten digit account number, and same the single digit card sequence number are concatenated, Kuhn's process yields the exact same result and thus does not produce a number of random binary bits.

Furthermore, contrary to the Examiner's assertion, there is nothing in the DES algorithm that ensures that each successive bit in an encryption result is equally likely and unpredictable or random. While this is a desired characteristic it is not necessarily a product of the DES algorithm.

For example, if the plaintext message "8787878787878787" is encrypted with the DES key "0E329232EA6D0D73", the result is the ciphertext "0000000000000000". (from "*The DES Algorithm Illustrated*" by J. Orlin Grabbe, copy attached)

Thus, Kuhn's process does not generate a number of random binary bits.

2.2 The Examiner also states that Kuhn's steps of writing the 64 bit cyphertext as a 16 bit hexadecimal number and examining digits 3-6 equates to Applicants' determining the least significant bits of the number of bits.

8

Applicants respectfully disagree because Matyas has no disclosure related to this feature and Kuhn specifically limits examination to digits 3-6 of the 16 digit hexadecimal number. Kuhn does not disclose selecting any 4 arbitrary digits but specifically states digits 3-6 are the digits to be considered, which are clearly not the least significant bits.

2.3 The Examiner further equates Kuhn's decimalizing digits 3-6 of the 16 digit hex number by substituting all occurrences of letters A-F with numbers 0-5 to Applicants' converting the least significant bits to a decimal integer.

Applicants disagree because the processes are clearly different and yield different results. Substituting all occurrences of letters A-F with numbers 0-5 in digits 3-6 of a hexadecimal number does not yield the same result as converting the least significant bits of a binary number to a decimal number. Applicants process is a mathematical conversion that produces a decimal equivalent of a binary number, while Kuhn describes a substitution or encoding process that does not yield a mathematical equivalent. Again, Matyas is silent with respect to this feature.

At least for these reasons, Applicants respectfully submit that independent claim 1 and dependent claims 2-12 are patentable over the combination of Kuhn and Matyas.

3. Applicants respectfully submit that claims 13-20 and 22-26 are patentable over the combination of Kuhn and Matyas in view of Holch et al. (US 6,280,328, "Holch").

The combination of Kuhn, Matyas, and Holch fails to disclose or suggest generating a number of random binary bits, determining the least significant bits of the number of bits, and converting

9

the least significant bits to a decimal integer, as recited by claim 13. Applicants fail to find these features in the cited combination.

At least for these reasons, the combination of Kuhn, Matyas, and Holch fails to render independent claim 13 and dependent claims 14-20 and 22-26 unpatentable.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Joseph V. Gamberdell, Jr   Date   2 August 2005
Reg. No. 44,695

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

10

CERTIFICATE OF FACSIMILE MAILING

I hereby certify that this correspondence is being transmitted by facsimile to 571-273-8300 on the date indicated below, addressed to the Commissioner of Patents, P.O. Box 1450, Alexandria VA 22313-1450.

Date: 8/2/2005   Signature: _____
                                    Person Making Deposit

11